Manage settings

SaaS Backup for Microsoft 365

NetApp
June 20, 2025

This PDF was generated from https://docs.netapp.com/us-en/saasbackupO365/concept_backup_policies.html on June 20, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Manage settings . . . 1
- Backup policies . . . 1
  - Backup policies for SaaS Backup provided storage . . . 1
  - Backup policies for BYOS . . . 1
- Backup settings . . . 1
  - Backup settings per service . . . 1
  - Update backup settings . . . 3
- Set notifications . . . 3
- Permissions . . . 4
  - Add additional service accounts . . . 4
  - Synchronize user permissions with Azure Active Directory . . . 4
  - Grant permissions to enable shared mailboxes . . . 5
- Role-based account access . . . 5
  - Assign administrative roles to user accounts . . . 5
  - Update administrative roles assigned to user accounts . . . 6
  - Delete all administrative roles from a user account . . . 6

Manage settings

Backup policies

SaaS Backup for Microsoft 365 has three predefined tiers of backup policies. These policy tiers vary in backup frequency and data retention period, depending upon whether you are using SaaS Backup provided storage or BYOS.

You can move data between the three policies, but you cannot create new policies or change the parameters of the predefined tiers.

Backup policies for SaaS Backup provided storage

Backup policy	Backup frequency	Default data retention period
Tier 1	Once every 12 hours	3 years
Tier 2	Once every 18 hours	3 years
Tier 3	Once every 24 hours	3 years

As an administrator, you can change the data retention period for SaaS Backup provided storage up to an unlimited period of time. SaaS Backup retains the backup data for the retention period if the subscription is active.

Backup policies for BYOS

BYOS is for existing customers only.

Backup policy	Backup frequency	Default data retention period
Tier 1	Once every 12 hours	Unlimited
Tier 2	Once every 18 hours	Unlimited
Tier 3	Once every 24 hours	Unlimited

Backup settings

You can update your backup settings to control various backup options. Available backup settings vary based on service.

Backup settings per service

Backup setting	Description	Enabled	Available in…
Auto Sync	Enables the automatic scheduled synchronization of newly added or deleted users, OneDrives, or site collections once every 24 hours.	By default	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft OneDrive for Business • Microsoft 365 Groups
Enable OneNote Backup	Enables the backup of OneNote notebooks.	Manually	• Microsoft SharePoint Online • Microsoft OneDrive for Business
Enable Restore of Recoverable Items	Enables the user to restore Microsoft Exchange recoverable items.	Manually	• Microsoft Exchange Online
Enable Backup of Recoverable Items	Enables the backup of Microsoft Exchange recoverable items. Only the tier 1 backup policy allows for the backup of recoverable items.	Manually	• Microsoft Exchange Online
Include Workflows	Includes workflows in the backup.	Manually	• Microsoft SharePoint Online • Microsoft 365 Groups
Include List Views	Includes list views in backup.	Manually	• Microsoft SharePoint Online • Microsoft 365 Groups

Backup setting	Description	Enabled	Available in…
Include Version History	Enables maintenance of multiple file versions in the backup. This setting only applies to individual files. It does not apply to entire folders, tiers, or services.	By default	• Microsoft SharePoint Online • Microsoft OneDrive for Business • Microsoft 365 Groups
Number of Versions	Sets the number of backup file versions to maintain. By default, the latest version is automatically backed up, even if this setting is not enabled.	Set to 20 by default	• Microsoft SharePoint Online • Microsoft OneDrive for Business • Microsoft 365 Groups

Update backup settings

Steps

1. Click **Services** from the left navigation pane.

2. Click Microsoft 365.

3. Under **Manage Services**, click the backup settings icon next to the service that you need to update. A list of your backup settings available for the selected service is displayed.
4. Select the desired backup settings.
5. Click **Confirm**.

Set notifications

You can add users to account notifications and then select the specific notifications you want each user to receive. For example, you can select to have a user receive an email notification each time there is a restore failure.

Steps

1. Click **ACCOUNT SETTINGS**.

2. Click **NOTIFICATION MANAGEMENT**.
3. Enter the email address of the account you want to receive notifications.
4. Click **Add Notifications**.
   The user is added under the list of accounts for notifications.
5. Select the specific notifications you want the user to receive.
6. Click **Save**.

Permissions

Add additional service accounts

If needed, you can add additional service accounts to improve backup performance. Service accounts are used to perform concurrent backups efficiently.

Steps

1. Log in to the Microsoft 365 Management Portal using an account with administrative privileges.
2. Click on the app launcher icon and then click **Admin**.
3. On the left, click **Users** and then **Active Users**.
4. Click **Add a User** to create a new account.
5. Fill in the form following the instructions below.
   - Use **Let me create the password**.
   - Deselect **Make this user change their password when they first sign in** option.
   - Select the role **Customized Administrator**.
   - Select **Exchange administrator** and **SharePoint administrator**.
   - Select **Create user without product License**.
6. For Exchange backups to run with newly created service accounts, assign the Exchange impersonation rights to these newly created service accounts.
   Configuring impersonations

SaaS backup automatically assigns the permissions on OneDrive and SharePoint sites, so you don't need to assign them.

You can enable multi-factor authorization (MFA) on this account.

Synchronize user permissions with Azure Active Directory

You can manually synchronize your user permissions with Azure Active Directory from within SaaS Backup for Microsoft 365.

Steps

1. Click

from the left navigation pane.
2. Click the Microsoft 365 link.

3. Click **Rediscover Permissions**.

If permissions for a services are discovered, the service is displayed with the option to active.

Grant permissions to enable shared mailboxes

You can grant permissions to enable shared mailboxes within NetApp SaaS Backup for Microsoft 365.

Steps

1. Click

from the left navigation pane.
2. Click the Microsoft 365 link.

3. Click **Grant Consent**.

You are redirected to the Azure authorization page for authentication.

4. Select your tenant account.
5. **Accept** the permissions.
Your shared mailboxes will be discovered during the next scheduled **Auto Sync** or you can perform a **Sync Now**. If you **Sync Now**, it will take a few minutes for your shared mailboxes to be discovered.
6. To access shared mailboxes after an **Auto Sync** or a **Sync Now** do the following:
   a. Click

from the left navigation pane.
   b. Click **Microsoft Exchange Online**.
   c. Click the number of unprotected mailboxes.
   d. Click the **Shared** tab.

Role-based account access

Assign administrative roles to user accounts

You can assign administrative roles to user accounts to grant administrative privileges to selected users for one or more services.

You can assign the following roles to users:

- Global Tenant: Grants administrative privileges to all services, storage target, and license updates (renewal/upgrade).
- Exchange Administrator: Grants administrative privileges to Microsoft Exchange Online only. Other services cannot be viewed or modified.
- OneDrive Administrator: Grants administrative privileges to Microsoft OneDrive for Business only. Other services cannot be viewed or modified.
- SharePoint Administrator: Grants administrative privileges to Microsoft SharePoint Online only. Other services cannot be viewed or modified.

Steps

1. Click the settings icon next to your user ID in the top left of the screen.
2. Click **ACCOUNT SETTINGS**.
3. Click **ROLE MANAGEMENT**.
4. Click the icon.
5. Enter the email address for the user you want to add.
6. Click the drop-down menu to select the role.
   You can assign one or more roles to a user.
7. Click **Confirm**.

Update administrative roles assigned to user accounts

If an update is made to a user's administrative roles, the user is automatically logged out of SaaS Backup for Microsoft 365. When the user logs back in, administrative role updates are reflected in the user's account.

Steps

1. Click the settings icon next to your user ID in the top left of the screen.
2. Click **ACCOUNT SETTINGS**.
3. Click **ROLE MANAGEMENT**.
4. Click **Update User** next to the user name that you want to update.
5. Click the drop-down menu to select the role.
   You can assign one or more roles to a user.
6. Click **Confirm**.

Delete all administrative roles from a user account

If all administrative roles are deleted from a user's account, the user is automatically logged out of SaaS Backup for Microsoft 365.

Steps

1.

Click the settings icon next to your user ID in the top left of the screen.

2. Click **ACCOUNT SETTINGS**.
3. Click **ROLE MANAGEMENT**.
4. Click **Delete User** next to the user name that you want to remove.
5. Click **Yes**.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.